Chapter

Discretization, the Road to Quantum Computing?

Jesús Lacalle

Abstract

The main challenge we face in making quantum computing a reality is error control. For this reason it is necessary to study whether the hypotheses on which the threshold theorem has been proved capture all the characteristics of quantum errors. The extraordinary difficulties that we find to control quantum errors effectively together with the little progress in this endeavor, compared to the enormous effort deployed by the scientific community and by companies and governments, should make us reflect on the road map to quantum computing. In this work we analyze error control in quantum computing and suggest that discrete quantum computing models should be explored. In this sense, we present a concrete model but, above all, we propose that Quantum Physics should be taken one step further, in order to allow discretization of the quantum computing model.

Keywords: quantum computing errors, quantum threshold theorem, discrete quantum computing errors, continuous quantum computing errors, discrete quantum computing, quantum physics

1. Introduction

Quantum computing is a multidisciplinary research area with extraordinary expectations in Computer Science [1, 2]. It proposes a radical change with respect to the classical computing model, moving to a quantum one. To do this, change the basic unit of classical information, the bit, for the quantum bit or qubit:

$$\begin{aligned} &\text{Bit}: \quad b \in \{0,1\} \quad \text{and} \\ &\text{Qubit}: \quad q \in \left\{ \alpha_0|0\rangle + \alpha_1|1\rangle \;\middle|\; \alpha_0, \alpha_1 \in \mathbb{C} \text{ and } |\alpha_0|^2 + |\alpha_1|^2 = 1 \right\}. \end{aligned} \tag{1}$$

The superposition principle of Quantum Physics makes the so-called quantum parallelism possible. Working with n qubits, quantum parallelism allows 2^n operations to be performed simultaneously. However, making this advantage effective by getting algorithms faster is a difficult challenge. Another important consequence of the superposition principle is the existence of entangled quantum states. The smallest entangled state is built with 2 qubits and is called an EPR pair, because it was first proposed by Einstein, Podolsky and Rosen in 1935:

$$q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2}$$

Another important feature of quantum computing is that it is a continuous computing model. Change a bit, which can only take two discrete values, for a qubit, which is a point on the 3−dimensional unit sphere centered at 0 in the real space $\mathbb{R}^4$. This fact makes quantum error control the main challenge for the feasibility of quantum computing. For this reason, one of the main research objectives in the 1990s was to solve this stumbling block. To address the problem, two fundamental tools were developed: quantum error correction codes [3–8] in combination with fault tolerant quantum computing [9–15].

The results obtained seemed to have theoretically solved the problem of quantum error control. The quantum threshold theorem or quantum fault-tolerance theorem was proved. This states that a quantum computer with a physical error rate below a certain threshold can, through application of quantum error correction schemes, suppress the logical error rate to arbitrarily low levels. Shor first proved a weak version [9] and the theorem was independently proven by the groups of Aharanov and Ben-Or [15], Knill, Laflamme and Zurek [13] and Kitaev [14].

All authors use the discrete errors introduced to define error-correcting quantum codes as a key element to prove the quantum threshold theorem. And they do it for two reasons: the constructed quantum codes allow correcting precisely those discrete errors and, even more important, any 1−qubit unitary matrix is a linear combination of those discrete errors. Indeed the discrete errors of a qubit are linear combinations of the well-known Pauli matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ and } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3}$$

However, recent studies [16, 17] indicate that fault-tolerant quantum computing does not cover all the loopholes through which quantum errors escape, accumulating during quantum computations. Lacalle, Pozo-Coronado, Fonseca de Oliveira and Martín-Cuevas model quantum errors as random variables, integrating the essentially continuous character of quantum errors. The first two authors obtain the formula for the variance of the sum of two independent quantum errors E_1 and E_2 [18]:

$$V(E_1 + E_2) = V(E_1) + V(E_2) - \frac{V(E_1)V(E_2)}{2}. \tag{4}$$

They prove it only for isotropic errors and conjecture that it is true in the general case. The n−qubits are represented by points on a $\left(2^{n+1} - 1\right)$−dimensional unit sphere $\mathcal{S}$ centered at 0 in the real space $\mathbb{R}^{2^{n+1}}$. Therefore, the variance of the quantum errors of the n−qubits, unlike what happens in $\mathbb{R}^n$, is bounded because the corresponding sphere is a closed and bounded set. In fact the variance always belongs to the interval $[0, 4]$.

The authors establish in [16, 17] that a quantum code fixes a quantum error if, assuming that the code's correcting circuit does not introduce new errors, the code reduces the variance of the quantum error. Despite these weak requirements, the authors find two types of quantum error that are not fixed by any quantum code. Let $\mathcal{C}$ be the quantum code used, Φ the pure quantum state that the n−qubit should have if no error occurs, Ψ the real quantum state of the n−qubit generated by the quantum error and $\tilde{\Phi}$ the code state resulting from applying the code correction circuit to the state Ψ, assuming that this circuit does not introduce new errors. From the point of view of the statistical study of errors, the disturbed state Ψ is a random variable on the sphere $\mathcal{S}$. The same holds for the state $\tilde{\Phi}$ resulting from the correction, in this case on the corresponding sphere of the subspace code of $\mathcal{C}$ (since

the accuracy of the correction circuit we are assuming implies that $\tilde{\Phi}$ belongs to $\mathcal{C}$). The variance of the quantum error is the expected value

$$V(\Psi) = E\left[\|\Phi - \Psi\|^2\right] \tag{5}$$

and the variance of the corrected state $V\left(\tilde{\Phi}\right) = E\left[\|\Phi - \tilde{\Phi}\|^2\right]$. Then $\mathcal{C}$ fixes the quantum error if:

$$V\left(\tilde{\Phi}\right) < V(\Psi). \tag{6}$$

The authors say in [16] that a quantum error Ψ is isotropic if its density function on the sphere $\mathcal{S}$ only depends on $\|\Phi - \Psi\|$ (θ_0, the first angle in polar coordinates). And they prove the following results:

1. If $\mathcal{C}$ detects an error the distribution of $\tilde{\Phi}$ is uniform ([16], Theorem 3).

2. $V\left(\tilde{\Phi}\right) \geq V(\Psi)$ for common probability distributions ([16], Theorem 5).

The first of the above properties indicates that if an error is detected in the code correcting circuit, all information has already been lost in computing. This result, despite being very negative from the point of view of quantum error control, is not surprising for isotropic errors.

The other type of quantum error studied by the authors in [17] is more important: qubit independent errors. They are much more difficult to analyze because they do not have as much symmetry as isotropic errors but they are errors that occur in real quantum computers. To facilitate the analysis, the authors focus on the $5-$qubit quantum code because of its high symmetry and argue that the behavior of this quantum code shows a general pattern. Although these two types of errors are very different (the dimension of the support of the isotropic errors is $2^{n+1} - 1$ while that of the qubit independent errors is much smaller: $4n$), the main results are surprisingly similar. In this case the authors prove the following results:

1. If $\mathcal{C}$ detects an error the distribution of $\tilde{\Phi}$ has central symmetry ([17], Theorem 4.2) and its variance is maximum ([17], Lemma 4.2).

2. $V\left(\tilde{\Phi}\right) \geq V(\Psi)$ for common probability distributions ([17], Theorem 4.4).

Note that the second property is the same for both types of quantum error. And, as regards the first, there is not much difference between a uniform distribution on a sphere and a centrally symmetric distribution, if they both approximate a point Φ on the sphere. Therefore, the results for both types of quantum error are similar and this fact is very striking.

Some reviewers have questioned the result of [17] for not considering that quantum states can be multiplied by a phase without physically changing their state. However, the authors of this work introduce the quantum variance that considers this fact,

$$V_q(\Psi) = E\left[\min_{\phi}\left(\|\Psi - e^{i\phi}\Phi\|^2\right)\right], \tag{7}$$

and relate it to the most common error measure in quantum computing, fidelity $F(\Psi)$:

$$1-\frac{V_q(\Psi)}{2}\leq F(\Psi)\leq\sqrt{1-\frac{V_q(\Psi)}{2}}. \tag{8}$$

These inequalities show that quantum variance and fidelity are essentially equivalent, since when quantum variance tends to 0, fidelity tends to 1 and, conversely, when fidelity tends to 1, quantum variance tends to 0. Of the three measures, the variance is the only one that allows to complete the complicated calculations performed in [17]. Furthermore, the authors state that the variance and the quantum variance have similar behaviors for continuous quantum computing errors. Indeed, let $\Phi=|0\rangle$ be a qubit and suppose that Φ is changed by error becoming the state $\Psi=W\Phi$, where W is the error operator given by Formula (5) in [17] whose density function $f(\theta_0)$ only depends on the angle θ_0. Then:

$$\begin{aligned}\Psi=&(\cos(\theta_0)+i\sin(\theta_0)\cos(\theta_1))|0\rangle+\\&(\sin(\theta_0)\sin(\theta_1)\cos(\theta_2)+i\sin(\theta_0)\sin(\theta_1)\sin(\theta_2))|1\rangle\end{aligned} \tag{9}$$

and, taking into account that

$$\min_{\phi}\left(\|\Psi-e^{i\phi}\Phi\|^2\right)=2-2|\langle\Psi|\Phi\rangle| \tag{10}$$

and the Eq. (5) we obtain:

$$V_q(X)=2-4\pi\int_0^{\pi}\left(1-\frac{\cos^2(\theta_0)}{2\sin(\theta_0)}\log\left(\frac{1-\sin(\theta_0)}{1+\sin(\theta_0)}\right)\right)\cdot f(\theta_0)\sin^2(\theta_0)d\theta_0 \text{ and}$$

$$V(X)=2-4\pi\int_0^{\pi}2\cos(\theta_0)\cdot f(\theta_0)\sin^2(\theta_0)d\theta_0.$$

We observe that the difference between the quantum variance and the variance are the weight functions of $f(\theta_0)\sin^2(\theta_0)$ in the integral and that they have a similar behavior for small errors, that is, for concentrated density functions $f(\theta_0)$ around $\theta_0=0$ (see **Figure 1**).

Even for large errors, for example a uniform distribution function $f=\frac{1}{2\pi^2}$, we have comparable values of the quantum variance and the variance:

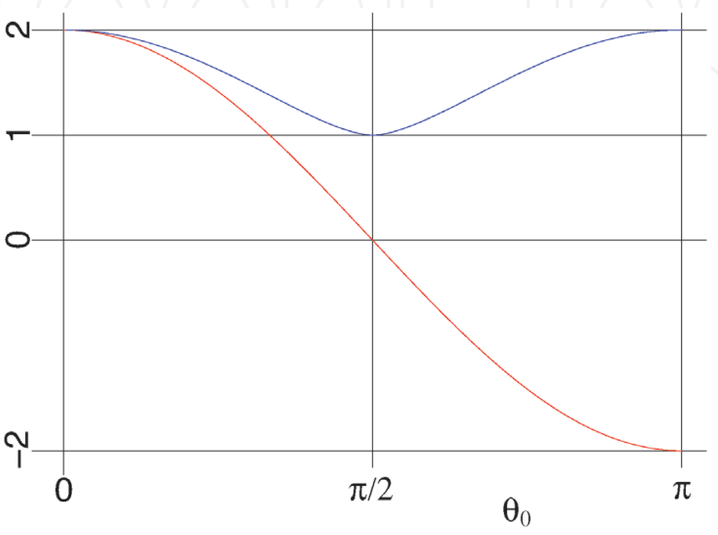

Figure 1.
Weight functions for quantum variance (red) and variance (blue).

$$V_q(\Psi) = \frac{2}{3} \text{ and } V(\Psi) = 2. \tag{11}$$

In [19], the study of isotropic errors is extended by analyzing the capacity of quantum codes to improve fidelity, and similar results to those presented in [16] are obtained: quantum codes do not improve the fidelity of uncoded quantum states for this type of error.

The results presented in [16, 17, 19] remind us that the quantum computing model is continuous and that the treatment of continuous quantum errors has many subtleties and it is an extraordinarily difficult challenge. Right now we are at a crossroads: extend fault-tolerant quantum computing to error models that include continuous errors or search for a discrete model of quantum computing that allows easier error control. The first road presents formidable difficulties: the fault-tolerant quantum architecture is based exclusively on discrete quantum errors and there is no analogical (continuous) system in the world comparable in complexity to a computer. The second one includes two processes: defining a discrete quantum computing model and finding a quantum system that allows the model to be implemented. It is difficult to know which of the two approaches will lead us to real quantum computing and, for this reason, both should be explored. In this work we study the second one.

A discrete quantum computing model has already been published [20] and, as far as we know, it is the first. In this work Gatti and Lacalle present a discrete quantum computing model based on the following basic requirements:

1. It describes real states in Quantum Physics.

2. It preserves the main characteristics of quantum states: superposition, parallelism and entanglement.

3. It allows to approximate general quantum states.

4. It contains simple quantum states.

Of all the possible sets of discrete quantum states, there is one that, fulfilling the first three properties, is the most outstanding in terms of simplicity of the states. It is the set of Gaussian coordinate states, which includes all the quantum states whose coordinates in the computation base, except for a normalization factor $\sqrt{2}^{-k}$, belong to the ring of Gaussian integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}. \tag{12}$$

To define the model they also need to introduce a set of quantum gates that verify the following properties: it contains quantum gates that transform discrete states into discrete states, and it generates all discrete quantum states. And they includes two elementary quantum gates that verify the above properties, H and G. The Hadamard gate H allows superposition, while the other one, G, is a $3-$qubit quantum gate. Two of them are control qubits, while the third is the target. If the control qubits are in state $|1\rangle$, then the quantum gate V is applied to the third qubit:

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{13}$$

This quantum gate allows the construction of all Gaussian coordinate states (discrete states) and it is because of this that they call it G.

This model of discrete quantum computing is related to Number Theory since discrete quantum states

$$\Phi = \frac{(a_0 + ib_0, a_1 + ib_1, \ldots, a_{2^n-1} + ib_{2^n-1})}{\sqrt{2}^{\,k}} \tag{14}$$

must verify the following diophantine equation:

$$a_0^2 + b_0^2 + a_1^2 + b_1^2 + \cdots + a_{2^n-1}^2 + b_{2^n-1}^2 = 2^k, \tag{15}$$

where $k \in \mathbb{N}$ and $a_0, b_0, \ldots, a_{2^n-1}, b_{2^n-1} \in \mathbb{Z}$. The above equation establishes deep connections between the discrete quantum computing model and Lagrange's four-square theorem. The same authors analyze this relationship in [21].

However, we must go one step further with the model of discrete quantum computing, so do not have the same error handling problem again. We need the discrete quantum states to have a basin of attraction associated with them so that any state that falls inside is automatically self-correcting, transforming into the discrete state. This process is used in the manufacture of hardware for classic computers with enormously satisfactory results.

However, Quantum Physics does not allow the application of this process. First of all, self-correction is not a one-to-one transformation and therefore cannot be unitary. And secondly, it cannot be the result of a quantum measurement either because the probability that the result was not the associated discrete state would be greater than zero. Consequently, we need Quantum Physics to go one step further to have the control that discrete quantum computing requires. Is this possible? We believe that this question should have an affirmative answer if the following one does: Is quantum computing possible?

In the following sections we develop further the ideas presented in this introduction.

2. Overview of quantum error control

Today's quantum error control has two essential components: quantum error correction codes [3–8] and fault-tolerant quantum computing [9–15]. There are textbooks on this subject, such as Gaitan's [22].

2.1 Quantum error correcting codes

Calderbank and Shor [3] and Steane [4] discovered an important class of quantum error correcting codes. The Calderbank-Shor-Steane (CSS) codes are constructed from two classical binary codes. Another approach to the subject originated the quantum stabilizer codes [5–8]. However, to better understand the role of quantum codes in correcting errors, a general description of them is more useful, without going into the detail of their internal structure.

An quantum error correcting code of dimension $[n, m]$ is a subspace $\mathcal{C}$ of dimension $d' = 2^m$ in the $n-$qubit space $\mathcal{H}^n$, whose dimension is $d = 2^n$. The $\mathcal{C}$ quantum code encoding function is a unitary operator C that satisfies the following properties:

$$C : \mathcal{H}^m \otimes \mathcal{H}^{n-m} \rightarrow \mathcal{H}^n \text{ and } \mathcal{C} = C(\mathcal{H}^m \otimes |0\rangle). \tag{16}$$

The $\mathcal{C}$ code fixes $d'' = 2^{n-m}$ discrete errors: E_0, E_1, $\ldots$, $E_{d''-1}$. Since the identity I should be among these unitary operators, we assume that $E_0 = I$. This process of

discretization of errors allows to correct any of them if the subspaces $S_s = E_s(\mathcal{C})$, $0 \leq s < d''$, satisfy the following property:

$$\mathcal{H}^n = S_0 \perp S_1 \cdots \perp S_{d''-1}. \tag{17}$$

That is, $\mathcal{H}^n$ is the orthogonal direct sum of said subspaces. Note also that $S_0 = E_0(\mathcal{C}) = I(\mathcal{C}) = \mathcal{C}$. In the stabilized code formalism, the code $\mathcal{C}$ is the subspace of fixed states of an abelian subgroup of the Pauli group $\mathcal{P}_n = \{\pm 1, \pm i\} \times \{I, X, Z, Y\}^n$ and discrete errors are operators of $\mathcal{P}_n$ that anti-commute with any of the subgroup generators, except for the identity operator E_0. If Formula (17) holds, the code is non-degenerate.

Suppose that a coded state Φ is changed by error, becoming the state Ψ. The initial state is a code state, that is, $\Phi \in S_0$, while the final state in general is not, that is, $\Psi \notin S_0$. If the disturbed state belongs to the subspace $W_\Phi = L(E_0\Phi, \ldots, E_{d''-1}\Phi)$, that is, if it is of the form

$$\Psi = \alpha_0 E_0 \Phi + \cdots + \alpha_{d''-1} E_{d''-1} \Phi \quad \text{with} \quad |\alpha_0|^2 + \cdots + |\alpha_{d''-1}|^2 = 1, \tag{18}$$

then the quantum code allows us to retrieve the initial state Φ. To achieve this, we measure Ψ with respect to the orthogonal decomposition of the Formula (17). The result will be $\frac{\alpha_s}{|\alpha_s|} E_s \Phi$ for a value s between 0 and $d'' - 1$. The value of s is called syndrome and allows us to identify the discrete error that the quantum measurement indicates. Then, applying the quantum operator E_s^{-1} we obtain $\frac{\alpha_s}{|\alpha_s|} \Phi$. This state is not exactly Φ but, differing only in a phase factor, both states are indistinguishable from the point of view of Quantum Mechanics. Therefore, the code has fixed the error.

An error that does not satisfy Formula (18), that is, it does not belong to W_Φ, cannot be fixed exactly. For example, if Ψ belongs to the code subspace $\mathcal{C}$, the error cannot be fixed at all since, being a code state, it is assumed that it has not been disturbed. Therefore it is important to analyze the limitation in the correction capacity of an arbitrary code, assuming that the code correction circuit does not introduce new errors.

Finally, we want to highlight that discrete errors can be chosen so that, for example, all errors affecting a single qubit are fixed. The best code with this feature that encodes one qubit is the 5-qubit quantum code [23, 24]. This code is optimal in the sense that no code with less than 5 qubits can fix all the errors of one qubit.

2.2 Fault-tolerant quantum computing

Fault-tolerant quantum computing was proposed with the aim of proving the quantum threshold theorem or quantum fault-tolerance theorem: a quantum computer with a physical error rate below a certain threshold can, through application of quantum error correction schemes, suppress the logical error rate to arbitrarily low levels. Shor first proved a weak version [9] and the theorem was independently proven by the groups of Aharanov and Ben-Or [15], Knill, Laflamme and Zurek [13] and Kitaev [14].

The essential elements of fault-tolerant quantum computing [9, 13, 15] are as follows: the encoding of each of the qubits with quantum error-correcting codes, the use of fault-tolerant quantum gates, the application of quantum gates on coded qubits (encoded operations) and the concatenation of quantum error-correcting codes.

Another essential element for the proof of the quantum threshold theorem is the quantum error model used. Shor [9] assumes that there is no decoherence error and

considers that in a quantum gate an error occurs with probability p and that the errors corresponding to different qubits are independent. Therefore the probability that errors will occur in k qubits simultaneously is:

$$\text{Prob}(k \text{ errors}) = \binom{n}{k}(1-p)^{n-k}p^k. \tag{19}$$

Knill, Laflamme and Zurek [13] and Aharanov and Ben-Or [15] consider both decoherence errors and errors in quantum gates and also assume the independence of errors on different qubits. The first [13] analyze quasi-independent and monotonic errors with error strength p and bound C: the total strength of the summands for which at least a given k many error locations have failed is at most Cp^k. Aharanov and Ben-Or [15] use density matrices and model the error in a qubit as follows:

$$(1-p)I + pE. \tag{20}$$

In all cases, the parameter p can be considered as the probability that an error occurs in a qubit and therefore the probability that k errors coincide in different qubits will be proportional to p^k. This consideration is key in proving the quantum threshold theorem and as such it appears in Gaitan's textbook [22] (see for example Table 1.1 on page 38). The errors associated with p are arbitrary and include what Shor calls "fast" errors and also "slow" errors. In particular they include the errors described by the Pauli matrices (3). This error model is the discretized quantum error model or the stochastic quantum error model.

The discretized quantum error model together with the concatenation of error-correcting quantum codes are the key elements in the proof of the quantum threshold theorem. The effect of the conjugation of both is as follows (see for example Figure 6 in [13]):

	Uncoded	Coded once	Coded twice
Number of qubits	1	7	49
Error probability	p	p^2	p^4

(21)

where we have used the 7−qubit CSS code. In each encoding the error in a qubit is fixed by the code and only errors of order 2 or greater remain. This scheme makes the error small, since p^k tends to zero if k grows.

But this approach cannot be used in all cases, for example for the decoherence error, since in this case the reality is different: the probability of errors occurring in all qubits is 1, although on the other hand the errors with high probability are small. In this situation the correcting code cannot handle a simultaneous error in all qubits and neither can it correct the "lower order" errors. Here is the essential difference between the discrete error model and the continuous one. The discrete error model does not fit this situation, in which small errors are not controlled and, after the application of the code correction circuit, become undetectable (because the resulting state belongs to the subspace code) and accumulate during computation.

Another key to fault-tolerant quantum computing is to avoid quantum gates that act on two qubits belonging to the same quantum code instance (implementation of fault-tolerant quantum gates for the used quantum code). In this way, the imprecision of the quantum gates only introduces error in at most one qubit of each instance of the quantum code. However, the error in 2−qubit quantum gates is not reduced to an error in each of the qubits. It also generates an error that affects both

qubits simultaneously (entangled error) and the code instances to which the two qubits belong are not designed to tackle it.

The use of an instance of an error correcting quantum code of dimension $[n, 1]$ on each of the qubits of a quantum circuit (algorithm) produces two additional effects to consider. First, this multiplies the number of qubits in the circuit by n. As a consequence, the decoherence per unit of time that occurs in the circuit is multiplied by n. Second, the number of gates in the circuit is multiplied by at least $n(n+1)$. Each encoded quantum gate requires a minimum of n quantum gates and, after each one of them, the code correction circuit must be applied, that is, at least another n quantum gates or measurements are needed. The effect of this increasing number of quantum gates is that the imprecision errors are multiplied by $n(n+1)$. A total of at least n^2 of these quantum gates and measurements correspond to the correction circuits and are therefore not protected. This fact remains even if we concatenate quantum codes in the last application of the error correcting code. If the number of quantum gates in an algorithm is n and the error correcting code is concatenated k times, the final number of gates is at least n^{2^k}. Then, the ratio of quantum gates not protected from imprecision errors is at least

$$1 - \frac{1}{n^{2^{k-1}}}. \tag{22}$$

Finally, it should be noted that the use of quantum codes produces an additional increase in decoherence by increasing the execution time of the algorithms.

Despite the difficulties raised above for the effective control of quantum errors, the discrete quantum error model or stochastic quantum error model allows the proof of the quantum threshold theorem. But unfortunately this model of quantum computing errors does not allow a realistic analysis of continuous quantum computing errors. These break the golden rule of error correction: all small errors must be corrected. The road of fault-tolerant quantum computing goes through including continuous errors in the quantum threshold theorem. This is a huge challenge and for this reason it is interesting to investigate other possible roads.

3. Discrete quantum computing

We are interested in discrete quantum computing because it could lead us to a quantum computing where error control was an easier challenge. In the literature there are some works on discrete quantum computing. They generally intend to simplify or better understand the quantum model: introducing modal concepts and finite fields for the representation of quantum amplitudes [25–29], using discretization for the design of algorithms [30], relating the structures of computation and the foundations of physics [31–38] and studying universal sets of discrete quantum gates [39–43].

As we have already commented in the Introduction, a discrete quantum computing model has already been published [20]. It is a model in which discretization is applied both to quantum states and to quantum gates and that aims to become independent from the standard quantum model (continuous model) and even, if possible, from continuous hardware (Quantum Physics). The presented discrete quantum computing model is based on the following basic requirements:

1. It describes real states in Quantum Physics.

2. It preserves the main characteristics of quantum states: superposition, parallelism and entanglement.

3. It allows to approximate general quantum states.

4. It contains simple quantum states.

Of all the possible sets of discrete quantum states, there is one that, fulfilling the first three properties, is the most outstanding in terms of simplicity of the states. It is the set of Gaussian coordinate states, which includes all the quantum states whose coordinates in the computation base, except for a normalization factor $\sqrt{2}^{-k}$, belong to the ring of Gaussian integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}. \tag{23}$$

To define the model the authors introduce a set of elementary quantum gates that verify the following properties: it contains quantum gates that transform discrete states into discrete states, and it generates all discrete quantum states. This set includes two quantum gates that verify the above properties, H and G. The Hadamard gate H allows superposition, while the other one, G, is a 3−qubit quantum gate. Two of them are control qubits, while the third one is the target. If the control qubits are in state $|1\rangle$, then the quantum gate V is applied to the third qubit:

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{24}$$

This model of discrete quantum computing is related to Number Theory since discrete quantum states

$$\Phi = \frac{(a_0 + ib_0, a_1 + ib_1, \ldots, a_{2^n-1} + ib_{2^n-1})}{\sqrt{2}^{\,k}} \tag{25}$$

must verify the following diophantine equation:

$$a_0^2 + b_0^2 + a_1^2 + b_1^2 + \cdots + a_{2^n-1}^2 + b_{2^n-1}^2 = 2^k, \tag{26}$$

where $k \in \mathbb{N}$ and $a_0, b_0, a_1, b_1, \ldots, a_{2^n-1}, b_{2^n-1} \in \mathbb{Z}$.

As we will see in the next subsection, the level of a discrete state is defined as the lowest natural number k for which the previous diophantine Eq. (26) holds. The superposition principle of Quantum Physics is satisfied in the following case: Given orthogonal discrete states $\Phi_0, \Phi_1, \ldots, \Phi_{j-1}$ belonging to levels $k_0, k_1, \ldots, k_{j-1}$ respectively, then the following linear combinations are also discrete quantum states:

$$\Phi = \frac{(c_0 + id_0)}{\sqrt{2^{k_0'}}}\Phi_0 + \frac{(c_1 + id_1)}{\sqrt{2^{k_1'}}}\Phi_1 + \cdots + \frac{(c_{j-1} + id_{j-1})}{\sqrt{2^{k'_{j-1}}}}\Phi_{j-1} \tag{27}$$

where $k_0', \; k_1', \; \ldots, \; k'_{j-1} \in \mathbb{N}$, $k_0 + k_0', k_1 + k_1', , k_{j-1} + k'_{j-1}$ have the same parity, $c_0, d_0, c_1, d_1, \ldots, c_{j-1}, d_{j-1} \in \mathbb{Z}$ and

$$\frac{c_0^2 + d_0^2}{2^{k_0'}} + \frac{c_1^2 + d_1^2}{2^{k_1'}} + \cdots + \frac{c^2_{j-1} + d^2_{j-1}}{2^{k'_{j-1}}} = 1. \tag{28}$$

The superposition principle is also satisfied for non-orthogonal discrete states. For example for the following two discrete states of level 4:

$$\Phi_0 = \frac{1}{4}(1+i, 1+2i, 0, 3)$$
$$\Phi_1 = \frac{1}{4}(1+i, 0, 1+2i, 3)$$
$$\Phi = \frac{5+9i}{8}\Phi_0 - \frac{3+9i}{8}\Phi_1. \tag{29}$$

Discrete state Φ has level 10, result of the sum of the levels of states Φ_0 and Φ_1, 4, and of coefficients used in the combination, 6.

3.1 Discrete quantum states

The quantum gates H and G, along with two auxiliary qubit (ancilla qubits), allow to perform a wide set of operations, for example, any permutation of the states of the computational base $\mathcal{B}$ and adding a factor -1, i or $-i$ to any subset of coordinates of an n-qubit, with respect to the computational base $\mathcal{B}$, where:

$$\mathcal{B} = [|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle, |8\rangle, \ldots, |2^n - 1\rangle] \text{ or}$$
$$\mathcal{B} = [|0\cdots00\rangle, |0\cdots01\rangle, |0\cdots10\rangle, |0\cdots11\rangle, \ldots, |1\cdots11\rangle]. \tag{30}$$

They also allow obtaining other quantum gates that are commonly used: X, $\Lambda X = Cnot$, $\Lambda^2 X = Toffoli$, Z, ΛZ, $\Lambda^2 Z$, V and ΛV.

The set of discrete quantum states $\mathcal{E}$ is defined as follows: $\mathcal{E}$ is the smallest set of quantum states which contains the computational base and is invariant under the application of the conforming gates H and G. As a consequence of the properties of H and G discussed above, the set $\mathcal{E}$ is also invariant by any permutation of coordinates and by the addition of a factor -1, i or $-i$ to any subset of coordinates.

The conforming quantum gates H and G have been chosen in order to generate exactly the states whose coordinates are Gaussian integers (except for a normalization factor of the form $\sqrt{2}^{-k}$ where $k \in \mathbb{N}$) that is, elements of the set $\mathbb{Z}[i]$ defined in Formula (23).

The set of Gaussian coordinate states E is defined by the following property: a quantum state $\Phi \in E$ if and only if there exists $k \in \mathbb{N}$ such that $\sqrt{2}^k \Phi \in \mathbb{Z}[i]^{2^n}$. And, as we have already commented before, the set of discrete states $\mathcal{E}$ and the set of Gaussian coordinate states E are the same. Consequently every discrete state must verify the Eq. (25), for a certain value $k \in \mathbb{N}$, and its coordinates without the normalization factor the diophantine Eq. (26).

Discrete states are classified by levels. We say that a discrete state Φ is at level $k \in \mathbb{N}$ if k is the smallest natural number for which it is verified that $\sqrt{2}^k \Phi \in \mathbb{Z}[i]^{2^n}$. From Eq. (25) it is concluded that there is a one-to-one relationship between the discrete states and the integer solutions of the Eq. (26) in which at least one component (real or imaginary part) of one coordinate is odd.

Given $k \in \mathbb{N}$, we call E_k to the set of discrete states of level k. These sets verify the following properties: for all $k \in \mathbb{N}$ E_k is finite, in fact its size is bounded by the number of solutions of the diophantine Eq. (26); and for all $k_1, k_2 \in \mathbb{N}$, $k_1 \neq k_2$, it holds $E_{k_1} \cap E_{k_2} = \varnothing$.

Given a number $k \in \mathbb{N}$, the set of discrete states with a level less than or equal to k, $E_{\leq k}$, allows us to approximate a general quantum state with a precision of the order of $\sqrt{2}^{-k}$. In this sense, the set of discrete states E allows us to approximate general quantum states and, as the level of the discrete states increases, the approximation is more precise. Finding the best approximation of a general quantum state through a discrete state in $E_{\leq k}$, $k \geq 0$, is a natural problem that allows us to relate

discrete quantum computing with quantum computing. This problem is also related to Number Theory because the discrete states must verify the diophantine Eq. (26).

In discrete quantum computing, the parity and the parity pattern of the coordinates are important. Given a coordinate $a+ib \in \mathbb{Z}[i]$ these concepts are defined as follows:

$$\begin{aligned} \mathrm{P}(a+ib) &= a+b \mod 2 \text{ and} \\ \mathrm{PP}(a+ib) &= (a \mod 2, b \mod 2). \end{aligned} \tag{31}$$

From formula (26) it is easy to deduce that the number of coordinates with parity 1 in a discrete state of level $k \geq 1$ is even.

The proof that the set of discrete states $\mathcal{E}$ is the same as the set of Gaussian coordinate states E illustrates well the structure of these sets and uses as key elements the concepts introduced above. The non-trivial part of this proof consists of giving a procedure (algorithm) to construct a state of E starting from a vector of the computational base, $|0\rangle$ for example, and applying the quantum gates H and G repeatedly. Gate H changes the level of all discrete state, most of the time increasing it by 1. But they also reduce by 1 the level of the states that we call "reducible". For example, the gate H applied to the nth-qubit, H_n, produces the following change in the discrete quantum state:

$$\begin{aligned} &\frac{1}{\sqrt{2}^k}(a_0+ib_0, a_1+ib_1, \ldots) \rightarrow \\ &\frac{1}{\sqrt{2}^{k+1}}((a_0+a_1)+i(b_0+b_1), (a_0-a_1)+i(b_0-b_1), \ldots). \end{aligned} \tag{32}$$

Therefore, for the state to be reducible, all the coordinates of the state resulting from the application of H_n must be multiples of 2. In this case, the initial increment by 1 of the discrete state level becomes a decrement by 1, by dividing the coordinates by 2. This division by 2 is compensated by multiplying the normalization factor $\sqrt{2}^{-(k+1)}$ by 2, that is, reducing its exponent by 2. Consequently, a state is reducible by applying H_n if its coordinates, taken two by two, have the same parity pattern:

$$\begin{aligned} \text{Pattern } (0,0): &\quad (even, even) \quad - \quad (even, even), \\ \text{Pattern } (0,1): &\quad (even, odd) \quad - \quad (even, odd), \\ \text{Pattern } (1,0): &\quad (odd, even) \quad - \quad (odd, even), \\ \text{Pattern } (1,1): &\quad (odd, odd) \quad - \quad (odd, odd). \end{aligned} \tag{33}$$

The proof starts from a discrete state of level $k \in \mathbb{N}$ and, applying the quantum gates H and G, its level is reduced, one by one, to level 0 and, once this is done, it is transformed into a state of the computational base. Then the construction of the state consists of writing this product of quantum gates in reverse order and substitute G for its inverse G^3. The keys of the proof are as follows. First, all the coordinates with the parity pattern $(0,1)$ are multiplied by i, so that all coordinates with parity 1 have the parity pattern $(1,0)$. Secondly, the coordinates are permuted so that the parity patterns $(1,0)$ appear at the end of the vector and, just before, the largest possible even number of patterns $(1,1)$ and the largest possible even number of patterns $(0,0)$.

If all the coordinates are already placed, the state is reducible. Otherwise the first two coordinates will have parity patterns $(0,0)$ and $(1,1)$ and the application of the quantum gate

$$R = V_1 H_n V_1 H_n, \tag{34}$$

where V_1 multiplies the second coordinate by i and H_n is the application of the quantum gate H to the last qubit, will solve the problem:

$$R\Phi = \frac{1}{\sqrt{2^k}}\left(\frac{a_0 - b_0 + a_1 + b_1}{2} + i\frac{a_0 + b_0 - a_1 + b_1}{2},\right.$$
$$\left.\frac{a_0 - b_0 - a_1 - b_1}{2} + i\frac{a_0 + b_0 + a_1 - b_1}{2}, a_2 + ib_2, \ldots\right). \tag{35}$$

The quantum gate R plays an important role in discrete quantum computing. It modifies (rotates) the parity patterns of the first two coordinates of the n-qubit as shown in **Figure 2**.

3.2 Discrete quantum gates

The introduced discrete quantum computing model satisfies some properties that the authors did not expect to hold. They define discrete quantum gates as the quantum gates that leave the set of discrete states invariant. This means that a quantum gate is discrete if applying it to any discrete state produces another discrete state as a result.

Discrete quantum gates are characterized by a simple property: a quantum gate is discrete if and only if the columns of its matrix, with respect to the computational base, are discrete states with levels of the same parity. This characterization is also fulfilled by substituting the columns of the matrix for the rows, since the matrix is unitary.

The number of discrete gates of one-qubit is finite because the number of discrete states of one-qubit is also finite: 8 discrete states of level 0, 24 of level 1, 16 of level 2 and none of level greater than or equal to 3. In this case all discrete gates can be generated from H and G.

Like discrete states, discrete gates are classified by levels. The level of a discrete gate is defined as the highest of the levels of its columns, considered as discrete

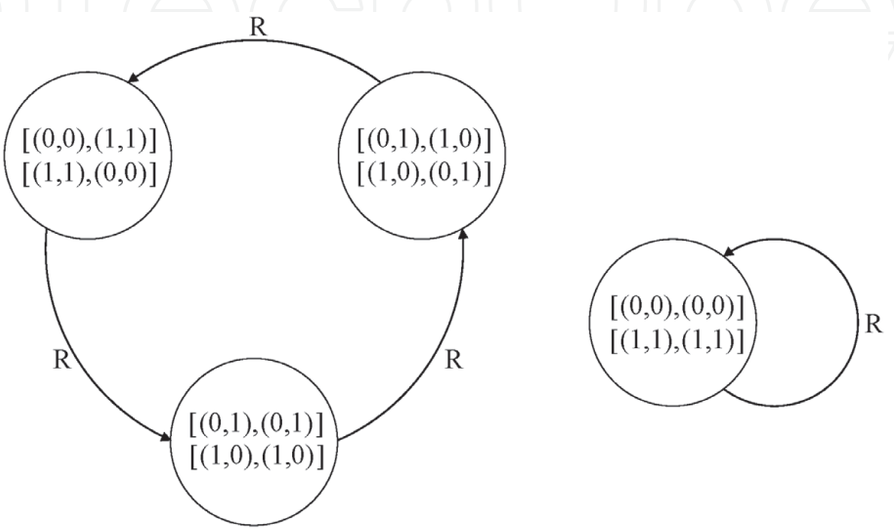

Figure 2.
Rotation of the parity patterns by the quantum gate R.

states. Obviously if we defined the level of a discrete gate using the rows instead of the columns, the result would be the same.

To proof that a discrete gate can be obtained as a product of gates H and G, it is enough to show that its level can be reduced, one by one, by left and right multiplying by these gates. This is possible only if we can make the discrete states of all its columns simultaneously reducible. And this surprisingly is possible!

Gatti and Lacalle prove it for discrete two-qubit quantum gates and conjecture that the result is true for any number of qubits. To do this, they generalize the properties of the parity patterns already introduced to the discrete gates (see **Figure 3**). They introduce the following concepts:

1. Simple match: Given two columns of a discrete gate, we will say that there is a simple match, when there exist elements in both columns, corresponding to the same row, with the real parts or the imaginary parts both odd.

2. Cross match: Given two columns of a discrete gate, we will say that there is a cross match, when there exist elements in both columns, corresponding to the same row, with the real part of one and the imaginary part of the other both odd.

From this definition and taking into account that the columns of a discrete gate are orthogonal discrete states, we can observe:

1. The number of odd elements in any column of a discrete gate is even.

2. Given two columns of a discrete gate, the number of simple matches and the number of cross matches are even.

We remark that every result about the columns of a quantum gate is also valid for the rows, since the matrix is unitary.

As it happened with the quantum states, we need to appeal to the gates R and R^t (transpose of R), which will act on the left and on the right, respectively. The gate R^t also produces a rotation of the coordinate parity patterns, analogously to the way R does (see **Figure 2**). However in this case the rotation is in the opposite direction.

The proof that discrete two-qubit quantum gates can be generated from gates H and G is much more technical than that described for discrete states. The parity constraints of the rows and columns of the discrete gates, derived from their unitarity, are sufficient tools to complete the proof. Readers interested in the details of this demonstration can refer to the original article [20]. The techniques used in the proof do not generalize for discrete gates of more than two qubits, but authors believe that the result is true in general.

Conjecture 1. For all $n \geq 3$ every dicrete n-qubit quantum gate can be decomposed into a product of H and G quantum gates.

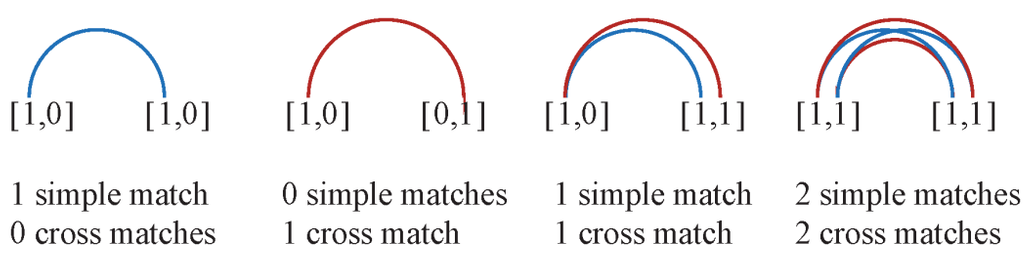

Figure 3.
Odd coordinate component matches.

4. Discrete quantum computing and Lagrange's four-square theorem

Conjecture 1 can be generalized as follows.

Conjecture 2. Given a set of $n-$qubit discrete states of levels of the same parity and orthogonal two by two, it is possible to build all of them simultaneously (applying a given circuit to different states of the computational base), using the conforming gates H and G.

Observe that the conjecture also makes sense for $2-$qubits, since in the previous subsection it has only been proved for sets of 4 discrete states. The conjecture is also interesting in the non-discrete case, since it asks about the possibility of simultaneously constructing up to 2^n quantum states simultaneously. In this case the conjecture is obviously true. Simply complete the orthonormal base, for example using the Gram-Schmidt method, and decompose the resulting unitary matrix into product of basic quantum gates. Therefore, it makes sense to ask if it is in the case of discrete quantum computing.

Before continuing, let us relax the discrete state level definition given in the previous section to any value of k for which the discrete state verifies Eq. (26). We will call these values *widespread levels*. Note that if k is a widespread level of a discrete state then $k+2$ is also. Then, a discrete state has widespread level k if and only if it is of the form k_0+2j, where k_0 is the level of the discrete state and j a natural number. This property allows to write all discrete states (with levels of the same parity) at the same widespread level.

Let us see that, somehow, building a set of orthogonal discrete states is equivalent to completing the set to an orthonormal base. For this reason we will focus in the following problem:

Problem 1. Given a natural number k and $\Psi_1, \ldots, \Psi_j$ $n-$qubit discrete states with widespread level k, $1 \leq j < 2^n$, such that $\langle \Psi_i | \Psi_m \rangle = 0$ for all $1 \leq i < m \leq j$, then is there an $n-$qubit discrete state with widespread level k, Ψ, such that $\langle \Psi_i | \Psi \rangle = 0$ for all $1 \leq i \leq j$?

Considering that every discrete $2-$qubit quantum gate can be built from gates H and G, the following can be easily proved: for $2-$qubits Conjecture 2 is true if and only if Problem 1 has an affirmative answer. Then the resolution of Problem 1 would allow us to build bases with special characteristics and it would help us to demonstrate the conjecture that any $n-$qubit discrete gate, with $n \geq 3$, can be generated from quantum gates H and G.

The fact that establishes the connection between discrete quantum computing and Lagrange's four-square theorem is that the discrete states have to satisfy Eq. (26). Lagrange's four-square theorem [44] says that every natural number is a sum of four squared integer numbers and, consequently, guarantees that there exist discrete states for any level $k \geq 0$ and for any number of qubits $n \geq 1$.

Problem 1 is an orthogonal version of Lagrange's four-square theorem, i.e. the discrete state Ψ must verify the Diophantine Eq. (26) and the following orthogonality conditions:

$$\langle \Psi_i | \Psi \rangle = 0 \quad \text{for all} \quad 1 \leq \mathrm{i} \leq \mathrm{j}. \tag{36}$$

Note that given a value of k, if the Eq. (26) has a solution for a $1-$qubit, then it has a solution for every number of qubits $n \geq 2$. Nevertheless, this generalization is not necessarily true for the Problem 1, because of orthogonality conditions. Therefore the problem has its own entity for any number of qubits n.

Problem 1 turns out to be a difficult question in Number Theory and has deep implications. For this reason we begin with the following simplification that most resembles Lagrange's four-square problem: $n = 2$, integers as coordinates instead of

Gaussian integers and normalization factor $\sqrt{p}$, being p a prime number, instead of $\sqrt{2^k}$.

Problem 2. Given a prime number p and $v_1, \ldots, v_k \in \mathbb{Z}^4$, $1 \leq k \leq 3$, such that $\|v_i\|^2 = p$ for all $1 \leq i \leq k$ and $\langle v_i | v_j \rangle = 0$ for all $1 \leq i < j \leq k$, then is there a vector $v = (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ such that $\langle v_i | v \rangle = 0$ for all $1 \leq i \leq k$ and $\|v\|^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$?

Given a natural number $1 \leq k \leq 4$ and a set of vectors $v_1, \ldots, v_k \in \mathbb{Z}^4$ such that $\|v_i\|^2 = p$ for all $1 \leq i \leq k$ and $\langle v_i | v_j \rangle = 0$ for all $1 \leq i < j \leq k$, we will say that $S = \{v_1, \ldots, v_k\}$ is a $p-$*orthonormal system* and, if $k = 4$, that S is a $p-$*orthonormal base*.

Given a $p-$*orthonormal system* S, we will call *support of* S, $supp(S)$, to $\{i \mid \exists j \ \{\text{such that the}\}\ i\text{-}\{\text{coordinate of}\}\ v_j \neq 0\}$ and we will say that $|supp(S)|$ is the *support size of* S.

In this context, the problem we are dealing with (Problem 2) is stated as follows: given a prime number p and a $p-$orthonormal system $S = \{v_1, \ldots, v_k\}$, $1 \leq k \leq 3$, prove that there exists $v \in \mathbb{Z}^4$ such that $\langle v_i | v \rangle = 0$ for all $1 \leq i \leq k$ and $\|v\|^2 = p$.

To prove the result, the authors consider four cases. Three of them are solved with basic linear algebra techniques. However the fourth case is much more difficult, and requires the use of lattices and some Number Theory results.

Case 1: one vector $p-$orthonormal systems.

If the $p-$orthonormal system S has a single vector $v_1 = (x_1, x_2, x_3, x_4)$, the solution (valid for all $p \geq 1$) is trivial: the required vector is, for example, $v = (x_2, -x_1, x_4, -x_3)$.

Case 2: two vectors $p-$orthonormal systems with support size 2.

If the $p-$orthonormal system S has two vectors with $|\text{supp}(S)| = 2$, the solution (valid for all $p \geq 1$) is as well trivial. Suppose, without loss of generality, that $\text{supp}(S) = \{1, 2\}$, $v_1 = (x_1, x_2, 0, 0)$ and $v_2 = (y_1, y_2, 0, 0)$. Then, the required vector is, for example, $v = (0, 0, x_1, x_2)$.

Case 3: three vectors $p-$orthonormal systems.

If the $p-$orthonormal system S has three vectors, their exterior product allows us to obtain the required vector (valid for all $p \geq 1$). It is enough to prove that all the coordinates of the exterior product are multiples of p and divide this vector by p to obtain the vector we are looking for.

So far, attempts to extend the proof of Problem 2 to arbitrary values of the natural number p have been unsuccessful, despite having been proven with a computer that the result is true up to $p = 10000$. This fact shows that the problem has a deep relationship with Number Theory. For discrete quantum computing the affirmative answer to Problem 1, as well as the proof of Conjectures 1 and 2, are very important. It would mean that discrete quantum computing maintains the most important properties relative to orthogonal and orthonormal vector systems and unitary transformations.

If we generalize Problem 2 by applying it to other dimensions, we see that counterexamples can be found for every dimension n that is not a multiple of 4. Thus, from Problem 2, we arrive at the following conjecture.

Conjecture 3. Given $n \equiv 0 \bmod 4$ ($n \geq 1$) and $p \geq 1$ and a $p-$orthonormal system in $\mathbb{Z}^n$, S, then S can be extended to a $p-$orthonormal base.

In all the problems raised and the conjectures established, the parities of the coordinates are important and, where appropriate, their parity patterns. It is also interesting to note that if we only want orthogonal systems, without specifying the norm or level of the vector with which we want to extend the system, all problems and conjectures are solved affirmatively.

Finally, we want to comment that the authors of the work in which discrete quantum computing is related to Lagrange's four-square theorem [21], conjecture that Problem 1 has an affirmative answer.

5. Does quantum physics allow discrete quantum computing?

Discrete quantum computing could in principle make error control easier. But in order to take advantage of the fact that quantum states are discrete, Quantum Physics must allow the construction of self-correcting systems. A system with these characteristics associates a basin of attraction with each discrete state so that whenever the $n-$qubit falls into said basin of attraction, the system automatically corrects it, transforming it into the associated discrete state. However, this process does not fulfill the Schrödinger equation because it is not unitary. And it cannot be the result of a quantum measurement either because the probability that the result was not the associated discrete state would not be zero. Then, how can Quantum Physics implement discrete quantum computing?

We believe that Quantum Physics can take one step further in the description of physical systems. Quantum Physics still fails to explain fundamental physical concepts, to the point that physicists as relevant as Feynman said "I think I can safely say that nobody understands quantum mechanics" and Quantum Mechanics has a reputation for being especially mysterious.

An example of a surprising result is the the no-cloning theorem [45–47], which states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state. This result of Quantum Physics contrasts with the self-reproducing systems of nature and is also derived from the Schrödinger equation, that predicts a unitary evolution of physical systems.

Quantum Physics has so far failed to explain the concepts for which it has acquired the fame of mysterious. We must assume that these mysteries are intrinsic to the nature of physical systems or that there is a road for Quantum Physics to explain them and open new paths for its development. Next we are going to analyze some of the less understandable concepts of Quantum Physics.

The first concept that is difficult to understand is the wave-particle duality. These concepts are inherently incompatible and nevertheless both are necessary to explain many results of Quantum Physics. If we assume that physical systems have a coherent physical description, we must conclude that elementary particles are neither waves nor particles. Therefore they must be something else.

On the other hand, the postulates of Quantum Physics introduce two processes to describe the evolution of physical systems: the Schrödinger equation and quantum measurements. The first predicts a unitary evolution of physical systems while the second seems to violate the prediction of the first. Many researchers assume that the result of the measurement of a quantum system is a random process whose probabilities depend on the measured system and not on the device that performs the measurement, and that the result is random, that is, there are no hidden variables that determine the result deterministically. In this interpretation the measurement process violates the Schrödinger equation. Other interpretations regard quantum states as statistical information about quantum systems, thus asserting that abrupt and discontinuous changes of quantum states are not problematic, simply reflecting updates of the available information. These reinforce the mysterious character of Quantum Physics and change its objective of describing physical systems for that of only obtaining information.

Finally, we want to comment on the interpretations made of the wave function obtained by solving the Schrodinger equation. It is common to hear that the wave function, for example of an electron, does not indicate that the particle is at all points where the wave function is not zero and that it is not an indicator of our ignorance of the position of the particle. On the one hand we give all the credit to the Schrödinger equation and on the other we take it away from the wave function.

As we see the controversy continues to haunt Quantum Physics. From our point of view, Quantum Physics has found a prediction system for the results of the measurements of physical systems, but it does not describe them. This prevents Quantum Physics from advancing in the deductive knowledge of physical systems, leaving only the advance based on experimentation. Does Quantum Physics really describe everything we can know about physical systems? We do not believe it.

What can be done to get out of this loop? We believe that we should focus on the initial problem: the wave-particle duality. As we have indicated before, this dilemma indicates that elementary particles are neither waves nor particles. Therefore the first objective is to determine its nature. To do this, we must look for questions that can be answered through the design of experiments and that shed light on the nature of elementary particles. In our opinion the first important question is the following: In how many points of space can an elementary particle be simultaneously?

Physics, in addition to the problems of Quantum Physics already mentioned, also has serious problems to combine two of its most notable theories: General Relativity and Quantum Physics. Undoubtedly, any theory that goes in the direction of discretizing space must also consider the discretization of time. In our study we only intend to contribute ideas so that Quantum Physics can overcome the controversies that it is not able to explain. We do not start from the hypothesis that Quantum Physics must be a discretized theory, but we believe that it must be a theory that allows self-correction and that this property must allow the implementation of a discrete quantum computation.

In Quantum Physics, different types of discretization have been proposed, in addition to the one presented in this article. Thus, in [48] a discretization of the quantum state space is proposed in order to explain Born's rule for probabilities. The proposal, despite being very similar to the one we have presented in this article, has very different objectives. In [48] it is used to try to explain two of the most important interpretations of Quantum Physics: Many Worlds and Copenhagen interpretation. In our case the objective is to define a discrete quantum computing model allowing effective control of quantum errors. And this objective leads us to pose an important question, aimed at explaining the wave-particle duality: In how many points of space can an elementary particle be simultaneously?

5.1 Hypothesis on the nature of elementary particles

Elementary particles cannot be in only one position in space because they cannot explain their behavior as waves. Then, in how many positions can they be simultaneously? The answer can be a finite number greater than one, a countable infinite number, or even an uncountable infinite number. Due to the principle of simplicity, we are inclined to take as a working hypothesis that the answer is a finite number greater than one.

And what does it mean for a particle to be simultaneously at various points in space? In our hypothesis the particle orbit between all its possible positions but being in only one at each time. Therefore simultaneity must be taken in a non-strict sense. That a particle orbits in different points means that it disappears from one point and appears in another and so on. The particle does not travel from one point to another through ordinary space and, in this sense, it may violate the special relativistic principle of speed limitation. Colloquially speaking the particle travels through a "wormhole", without deforming space through large concentrations of mass.

And, why do we choose this elementary particle model as a hypothesis? Because as we have said, the particle must be able to be in more than one point simultaneously and there are already experimental results of quantum nonlocality [49–53]. As far as we know, quantum nonlocality does not allow for faster-than-light communication and it is generally assumed that is compatible with special relativity and its universal speed limit of objects. We believe that quantum nonlocality in some sense violates the aforementioned principle of special relativity. We do not believe that the physical characteristics of the systems should be subordinated to the ability to transmit information.

From our point of view, the multi-position structure of the particles generates nonlocality in the usual space and breaks its Euclidean behavior. In this way physical systems can interact non-locally in space through their multi-position structure.

Another question that arises naturally from our working hypothesis is how scattered can the points that define an elementary particle be in space? Non-point particles can naturally explain their intrinsic angular momentum and this, in turn, give us information about the structure of the particles. For example, a particle that could be in three points in space would have an angular momentum proportional to the area of the triangle determined by its positions. This would indicate that the dispersion of the particles would occur on typical scales of Quantum Physics.

The multi-position particle hypothesis would again bring up some problems that originated Quantum Theories, such as, for example, the stability of atoms. This problem would be solved by the spatial scattering of the electrons around the nucleus. In this case the far electromagnetic field generated by the electrons would decrease faster than the inverse of the square of the distance and this would prevent the electrons from losing their energy in the form of electromagnetic radiation.

Our hypothesis would force us to readapt Quantum Theory. Therefore, we should plan experiments that allow us to contrast it. Is this possible?

5.2 How to test the hypothesis experimentally?

We would like to propose a couple of experiments that could theoretically provide information on our hypothesis about the structure of elementary particles. The first is a variation of the flagship experiment in which the wave-particle duality

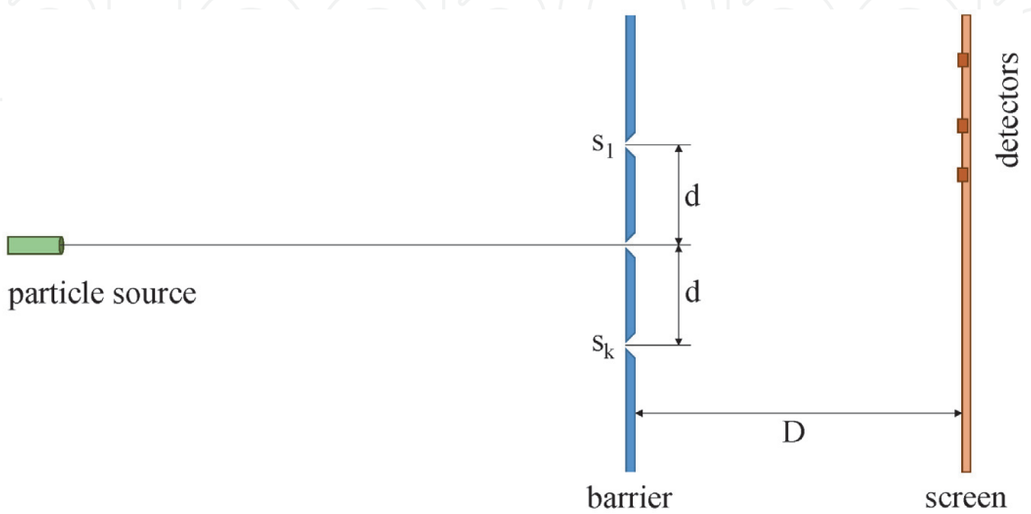

Figure 4.
k-slit experiment.

of elementary particles is tested: the double-slit experiment. The second uses a known quantum effect: the quantum tunneling.

Experiment 1. ***k*-slits.** We launch, one by one, elementary particles towards a barrier orthogonal to the direction of the movement of the particles (see **Figure 4**). In the barrier there are k parallel slits at a distance d one from the following: $s_1, s_2, \ldots, s_k$. Behind we place a screen parallel to the barrier and at a distance D from it. On this screen we place the detectors to obtain the interference pattern of the particles.

The objective of this experiment is to determine if the particles, according to our hypothesis, can be simultaneously in exactly $k-1$ positions. If this hypothesis is true, a particle cannot pass through the k slits. It can pass through $k-1$ slits at most. Therefore, the interference pattern will depend on whether the hypothesis is true.

We start the experiment by choosing $k=3$. If the hypothesis that the particles are in exactly $k-1$ positions simultaneously is not corroborated, we increase the value of k by 1 and carry out the experiment again. And when is our hypothesis confirmed? When the interference pattern obtained is $P(\text{true})$ instead of $P(\text{false})$:

1. $P(\text{true}) = \frac{P(s_1, \ldots, s_{k-1}) + P(s_1, \ldots, s_{k-2}, s_k) + \cdots + P(s_2, \ldots, s_k)}{k}$.

2. $P(\text{false}) = P(s_1, s_2, \ldots, s_k)$.

It would be necessary to estimate if the measurements can be precise enough to distinguish the two patterns and, in the first, if the probability of the k possible cases is the same or not.

Experiment 2. Quantum tunneling. We launch, one by one, elementary particles towards a potential barrier orthogonal to the direction of the movement of the particles (see **Figure 5(a)**). The energy of the particles is insufficient to jump the potential barrier and its width is small enough to allow the particles to have an appreciable probability of passing the barrier by tunneling. The particles are prepared in two different states. In the first state the intrinsic angular momentum of the particles is parallel to the direction of motion and, in the second state, it is orthogonal.

The objective of this experiment is to determine if the state of the particles influences the probability of quantum tunneling. If this influence is confirmed, it would mean that the orientation of the intrinsic angular momentum of the particles determines in some way the internal structure of the particle against the potential barrier. This could be explained quite understandably with the hypothesis that the particles are in exactly 3 positions at the same time. In this case the particle is always in a plane and the intrinsic angular momentum can orient that plane. If the three

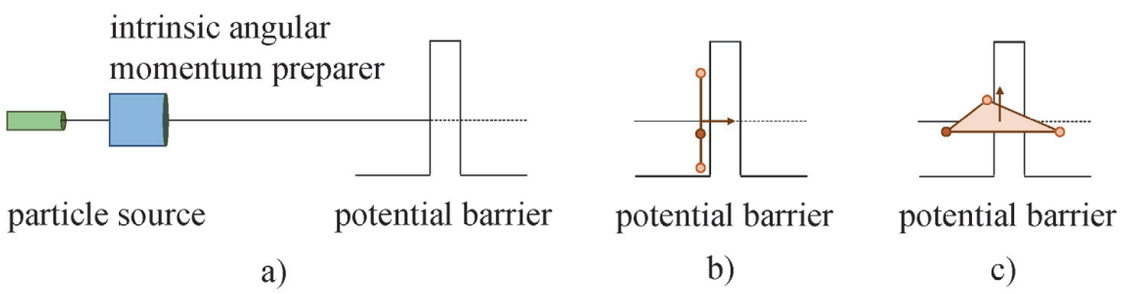

Figure 5.
Quantum tunneling experiment.

positions that define the particle reach the barrier simultaneously, the particle will not be able to pass (see **Figure 5(b)**). But if one of the positions arrives earlier, this position could cross the barrier while the particle orbits in the other positions (see **Figure 5(c)**). Thus, when the particle orbits in this position it will already be on the other side of the barrier.

We believe that it is not difficult to design more experiments that can shed light on our hypothesis of elementary particles. At this moment we are studying the dynamics of these multi-position particles.

6. Conclusions

In this article we introduce the discrete quantum computing as an alternative road to real quantum computing. The discrete quantum computing model is of great interest in itself both because, while maintaining all the important properties of quantum computing, it is an especially simplicity model and because error control is theoretically easier in this model. The introduced discrete quantum computing model satisfies some surprising properties that the authors believed would not hold and has deep connections to Number Theory.

The reason we set out on this alternative road to quantum computing is because error control in quantum computing is an extremely difficult challenge. The fact that the quantum computing model is continuous means that the golden rule of error control cannot be used: small errors are exactly corrected. A quantum computer is a very complex system from the point of view of error control. It allows reaching any quantum state (solution to the instance of a problem) by any path (algorithm). Doing this while keeping the error (entropy?) controlled is certainly an impressive challenge. As a consequence of the difficulty of controlling errors in continuous systems, there is no analog (continuous) device remotely comparable in operational complexity to a computer.

However, Quantum Physics does not allow the implementation of a discrete quantum computing model that allows self-correction of errors. To overcome this difficulty we ask Quantum Physics to go one step further in describing physical systems, beyond the prediction of measurement results. For this we propose a hypothesis about the nature of elementary particles that tries to overcome the never-understandable principle of wave-particle duality.

Summarizing, we propose an alternative road to quantum computing that passes through the discretization of this computing model and overcoming the interpretation gaps of Quantum Physics relative to the physical systems.

Author details

Jesús Lacalle
Universidad Politécnica de Madrid, Madrid, Spain

*Address all correspondence to: jesus.glopezdelacalle@upm.es

References

[1] Marella S T, Parisa H S K. Introduction to Quantum Computing. In: IntechOpen. DOI: 10.5772/intechopen.94103. Available from: https://www.intechopen.com/online-first/introduction-to-quantum-computing

[2] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge University Press; 2010. 664 p. DOI: 10.1017/CBO9780511976667

[3] Calderbank A R, Shor P W. Good quantum error-correcting codes exist. Phys. Rev. A. 1996;54:1098–1105.

[4] Steane A M. Multiple particle inference and quantum error correction. Proc. Roy. Soc. A. 1996;452:2551.

[5] Gottesman D. Class of quantum error correcting codes saturating the quantum Hamming boud. Phys. Rev. A 1996;54:1862.

[6] Calderbank A R, Rains E M, Shor P W, Sloane N J *A. quantum* Error Correction and Orthogonal Geometry. Phys. Rev. Lett. 1997;78:405.

[7] Gottesman D. Stabilizer Codes and Quantum Error Correction [thesis]. California Institute of Technology; 1997.

[8] Calderbank A R, Rains E M, Shor P W, Sloane N J *A. quantum* error correction via codes over GF(4). IEEE Trans. Inf. Theory. 1998;44(4):1369–1387.

[9] Shor P W. Fault-tolerant quantum computation. In: Proceedings of 37th Conference on Foundations of Computer Science; 14-16 October 1996; Burlington, VT, USA. IEEE Comput. Soc. Press; 1996. p. 56–65. arXiv:quant-ph/9605011. DOI: 10.1109/SFCS.1996.548464.

[10] Steane A M. Active stabilization, quantum computation and quantum state synthesis. Phys. Rev. Lett. 1997;78:2252.

[11] Preskill J. Reliable quantum computers. Proc. Roy. Soc. Lond. A. 1998;454:385–410.

[12] Gottesman D. Theory of fault-tolerant quantum computation. Phys. Rev. A. 1998;57:127–137.

[13] Knill E, Laflamme R, Zurek W H. Resilient Quantum Computation. Science. 1998;279(5349):342–345. arXiv:quant-ph/9702058v1. DOI: 10.1126/science.279.5349.342

[14] Kitaev A Yu. Fault-tolerant quantum computation by anyons. Annals of Physics. 2003;303(1):2–30. arXiv:quant-ph/9707021. DOI: 10.1016/S0003-4916(02)00018-0

[15] Aharonov D, Ben-Or M. Fault-Tolerant Quantum Computation with Constant Error Rate. SIAM Journal on Computing. 2008;38(4):1207–1282. arXiv:quant-ph/9906129. DOI: 10.1137/S0097539799359385

[16] Lacalle, J., Pozo-Coronado, L.M., Fonseca de Oliveira, A.L., Quantum codes do not fix isotropic errors. Quantum Inf Process 20, 37 (2021). https://doi.org/10.1007/s11128-020-02980-3.

[17] Lacalle J, Pozo Coronado L M, Fonseca de Oliveira A L, Martín-Cuevas R. Quantum codes do not fix qubit independent errors. Will appear in American Journal of Information Science and Technology. 2021. arXiv: 2101.03971 [quant-ph]

[18] Lacalle J, Pozo Coronado L M. Variance of the sum of independent quantum computing errors. Quantum Information & Computation. 2019;19(15-16):1294–1312. DOI: 10.26421/QIC19.15-16.

[19] Lacalle J, Pozo Coronado L M, Fonseca de Oliveira A L, Martín-Cuevas R. Quantum codes do not increase fidelity against isotropic errors. Personal communication 2021. It will appear in arXiv [quant-ph]

[20] Gatti L N, Lacalle J. A model of discrete quantum computation. Quantum Inf Process. 2018;17(192). DOI: 10.1007/s11128-018-1956-0

[21] Lacalle J, Gatti L N. Discrete quantum computation and Lagrange's four-square theorem. Quantum Inf Process. 2020;19(34). DOI: 10.1007/s11128-019-2528-7

[22] Gaitan F. Quantum error correction and fault tolerant quantum computing, CRC Press; 2008. 292 p.

[23] Bennet C H, DiVincenzo D P, Smolin J A, Wootters W K. Mixed state entanglement and quantum error correction. Los Alamos Physics Preprint Archive. 1999. arXiv:9909058 [quant-ph].

[24] Laflamme R, Miquel C, Paz J-P, Zurek W H. Perfect quantum error correction codes. Phys. Rev. Lett. 1996; 77:198. arXiv:9602019 [quant-ph].

[25] Benjamin S, Westmoreland M D. Modal quantum theory. Found. Phys. 2012;42(7):918-–925.

[26] Ellerman D. Quantum mechanics over sets. arXiv:1310.8221v1 [quant-ph].

[27] Hanson A J, Ortiz G, Sabry A, Tai Y-T. Geometry of discrete quantum computing. J. Phys. A Math. Theor. 2013;46(18):185301.

[28] Hanson A J, Ortiz G, Sabry A, Tai Y-T. Discrete quantum theories. J. Phys. A Math. Theor. 2014;47(11):115305.

[29] Gatti L N, García-López J. Geometría de estados discretos en computación cuántica. In: 10th Andalusian Meeting on Discrete Mathematics; July 10-11, 2017; La Línea de la Concepción, Cádiz, Spain.

[30] Chandrashekar C M, Srikanth R, Laflamme R. Optimizing the discrete time quantum walk using a su(2) coin. Phys. Rev. A. 2008;77:032326.

[31] Lloyd S, Dreyer O. The universal path integral. Quant. Inf. Process. 2016; 15(2):959–967.

[32] Long G-L. General quantum interference principle and duality computer. Commun. Theor. Phys. 2006; 45(5):825.

[33] Long G-L, Liu Y. Duality computing in quantum computers. Commun. Theor. Phys. 2008;50(6):1303.

[34] Long G-L, Liu Y, Wang C. Allowable generalized quantum gates. Commun. Theor. Phys. 2009;51(1):65.

[35] Gudder S. Mathematical theory of duality quantum computers. Quant. Inf. Process. 2007;6(1):37–48.

[36] Long G-L. Mathematical theory of the duality computer in the density matrix formalism. Quant. Inf. Process. 2007;6(1):49–54.

[37] Wei S-J, Long G-L. Duality quantum computer and the efficient quantum simulations. Quant. Inf. Process. 2016;15 (3):1189–1212.

[38] Lomonaco S J. How to build a device that cannot be built. Quant. Inf. Process. 2016;15(3):1043–1056.

[39] Kitaev A Y, Shen A, Vyalyi M N. Classical and Quantum Computation. American Mathematical Society. Providence; 2002;47.

[40] Oscar B P, Mor T, Pulver M, Roychowdhury V, Vatan F. On universal and fault-tolerant quantum computing: a novel basis and a new

constructive proof of universality for shor's basis. In: 40th Annual Symposium on Foundations of Computer Science; October, 17-19,1999; New York City, NY, USA.

[41] Shi Y. Both toffoli and controlled-not need little help to do universal quantum computing. Quant. Inf. Comput. 2003;3(1):84–92.

[42] Aharonov D. A simple proof that Toffoli and Hadamard are quantum universal. arXiv:0301040] [quant-ph].

[43] Kliuchnikov V, Maslov D, Mosca M. Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. Quant. Inf. Comput. 2013;13(7–8):607–630.

[44] Lagrange J L. Démonstration d'un théorème d'arithmétique, Oeuvres complétes **3**; 1869. 189–201

[45] Park J. The concept of transition in quantum mechanics. Foundations of Physics. 1970;1(1):23–33. DOI: 10.1007/BF00708652

[46] Wootters W, Zurek W. A Single Quantum Cannot be Cloned. Nature. 1982;299(5886):802–803. DOI: 10.1038/299802a0

[47] Dieks D. Communication by EPR devices. Physics Letters A. 1982;92(6): 271–272. DOI: 10.1016/0375-9601(82)90084-6

[48] Buniy R V, Hsua S D H, Zee, A. Discreteness and the origin of probability in quantum mechanics. Physics Letters B. 2006;640: 219–223. DOI: 10.1016/j.physletb.2006.07.050

[49] Aspect A, Dalibard J, Roger G. Experimental Test of Bell's Inequalities Using Time- Varying Analyzers. Physical Review Letters. 1982;49(25): 1804–1807. DOI: 10.1103/PhysRevLett.49.1804

[50] Rowe M, Kielpinski D, Meyer V et al. Experimental violation of a Bell's Inequality with efficient detection. Nature. 2001;409(6822):791–794. DOI: 10.1038/35057215

[51] Hensen B, Bernien H, Dréau A et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. Nature. 2015;526(7575):682–686. DOI: 10.1038/nature15759

[52] Giustina M, Versteegh M A M et al. Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons. Physical Review Letters. 2015;115(25): 250401. DOI: 10.1103/PhysRevLett.115.250401

[53] Shalm L K, Meyer-Scott E et al. (December 2015). Strong Loophole-Free Test of Local Realism. Physical Review Letters. 2015;115(25):250402. DOI: 10.1103/PhysRevLett.115.250402.